(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000101567 A**

(43) Date of publication of application: **07.04.00**

(51) Int. Cl **H04L 9/26**
G09C 1/00

(21) Application number: **10263681**

(22) Date of filing: **17.09.98**

(71) Applicant: **TOYO COMMUN EQUIP CO LTD**

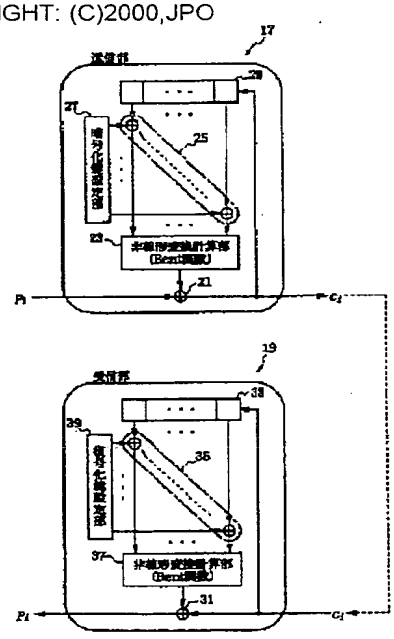
(72) Inventor: **SUGIMOTO KOICHI**

(54) CIPHERING AND DECIPHERING DEVICE AND METHOD THEREFOR

(57) Abstract:

PROBLEM TO BE SOLVED: To make cross correlation extremely small in the case of comparing a sequence in the case of deciphering the sequence of a cipher sentence by a certain key by a different key with the sequence of a plain sentence and to easily set a key.

SOLUTION: This device is provided with the first shift register 29 of plural stages operated in synchronism with synchronizing signals, the nonlinear transformation calculation part 23 of multi-bit input and 1-bit output, a cipher key setting part 27, an exclusive OR means 25 for exclusively ORing a cipher key set in the cipher key setting part to the register value of the shift register for respective bits and supplying it to the nonlinear transformation calculation part and the exclusive OR means 21 for exclusively ORing the plain sentence and the output of the nonlinear transformation calculation part for the respective bits. The nonlinear transformation calculation part is provided with the Boolean function computation means of the multi-bit input and 1-bit output called as a Bent function.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－101567
（Ｐ2000－101567Ａ）
(43)公開日　平成12年４月７日(2000.4.7)

(51)Int.Cl.'		識別記号	Ｆ Ｉ			ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ	9/26		Ｈ０４Ｌ	9/00	６５９	５Ｊ１０４
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ｄ	

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願平10－263681

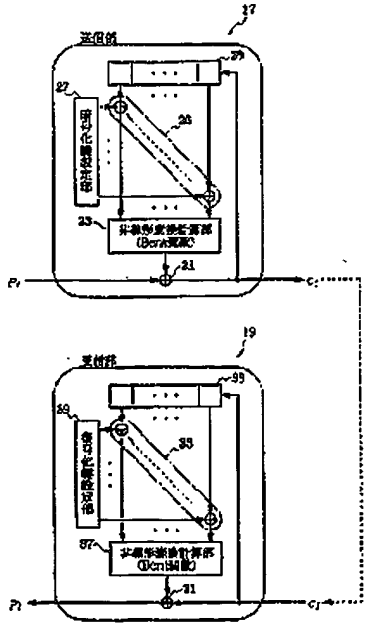
(22)出願日　平成10年９月17日(1998.9.17)

(71)出願人　000003104
東洋通信機株式会社
神奈川県高座郡寒川町小谷２丁目１番１号
(72)発明者　杉本　浩一
神奈川県高座郡寒川町小谷二丁目１番１号
東洋通信機株式会社内
(74)代理人　100085660
弁理士　鈴木　均

Ｆターム(参考)　5j104 AA01 AA18 JA06 NA02 NA08
NA23

(54)【発明の名称】　暗号化及び復号化装置とその方法

(57)【要約】　（修正有）
【課題】　ある鍵による暗号文の系列を異なる鍵で復号した場合の系列を、平文の系列と比較した場合、相互相関が極めて小さく、かつ、鍵の設定を容易にする。
【解決手段】　同期信号に同期して動作する複数段の第１のシフトレジスタ２９と、多ビット入力１ビット出力の非線形変換計算部２３と、暗号化鍵設定部２７と、シフトレジスタのレジスタ値に対して上記暗号化鍵設定部に設定された暗号化鍵をビット毎に排他的論理和演算して非線形変換計算部へ供給する排他的論理和演算手段２５と、平文と非線形変換計算部の出力とをビット毎に排他的論理和演算する排他的論理和演算手段２１とを具備し、非線形変換計算部はＢｅｎｔ関数と呼ばれる多ビット入力１ビット出力のブール関数演算手段を備える。



1

【特許請求の範囲】

【請求項１】　伝送情報（平文）を暗号化する暗号化装置であって、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力１ビット出力の非線形変換計算部と、暗号化鍵設定部と、上記シフトレジスタの一部もしくは全部のレジスタ値に対して上記暗号化鍵設定部に設定された暗号化鍵をビット毎に排他的論理和演算して上記非線形変換計算部へ供給するための第１の排他的論理和演算手段と、上記平文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算するための第２の排他的論理和演算手段とを具備し、

上記非線形変換計算部は、少なくともＢｅｎｔ関数と呼ばれる多ビット入力１ビット出力のブール関数演算手段を備えたものであり、暗号文が、上記平文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算することによって得られ、その暗号文が、同時に上記シフトレジスタに入力される構成となっていることを特徴とする自己同期型ストリーム暗号化装置。

【請求項２】　暗号文を復号化する復号化装置であって、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力１ビット出力の非線形変換計算部と、復号化鍵設定部と、上記シフトレジスタの一部もしくは全部のレジスタ値に対して上記復号化鍵設定部に設定された復号化鍵をビット毎に排他的論理和演算して上記非線形変換計算部へ供給するための第１の排他的論理和演算手段と、上記暗号文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算するための第２の排他的論理和演算手段とを具備し、

上記非線形変換計算部は、少なくともＢｅｎｔ関数とよばれる多ビット入力１ビット出力のブール関数演算手段を備えたものであり、上記暗号文が、上記シフトレジスタに入力され、同時に、平文が、先の暗号文と非線形変換計算部からの出力とをビット毎に排他的論理和演算を施すことによって得られることを特徴とする自己同期型ストリーム復号化装置。

【請求項３】　伝送情報（平文）を暗号化する暗号化方法であって、同期信号に同期して動作する複数段のシフトレジスタの一部もしくは全部のレジスタ値に対して暗号化鍵設定部に設定された暗号化鍵を第１の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、

少なくともＢｅｎｔ関数と呼ばれる多ビット入力１ビット出力のブール関数演算手段を備えた非線形変換計算部によって上記第１の排他的論理和演算手段よりの値を非線形変換するステップと、

上記平文と上記非線形変換計算部からの出力とを第２の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、

上記暗号文を上記シフトレジスタに入力するステップとを具備することを特徴とする自己同期型ストリーム暗号化方法。

2

【請求項４】　暗号文を復号化する復号化方法であって、同期信号に同期して動作する複数段のシフトレジスタの一部もしくは全部のレジスタ値に対して復号化鍵設定部に設定された復号化鍵を第１の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、

少なくともＢｅｎｔ関数とよばれる多ビット入力１ビット出力のブール関数演算手段を備えた非線形変換計算部によって上記第１の排他的論理和演算手段よりの値を非線形変換するステップと、

上記暗号文と上記非線形変換計算部からの出力とを第２の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、

上記暗号文を、上記シフトレジスタに入力するステップとを具備することを特徴とする自己同期型ストリーム復号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、伝送情報（平文）を暗号化して通信する暗号通信システムに関し、特に、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と平文の系列とを比較した場合、その相互相関が極めて小さくなり、かつ、鍵の設定が容易となる自己同期型ストリーム暗号方式の暗号通信システムにおける暗号化及び復号化装置とその方法に関する。

【０００２】

【従来の技術】従来より、電話機や無線通信装置やデータ通信装置等における暗号通信システムにおいては、その暗号通信システムの両端の通信当事者以外の第三者がその暗号通信システムで伝送される情報を知ることができないようにするために、その暗号通信システムで伝送される伝送情報を暗号化することが行われている。この暗号化の方式としては多種の方式が知られているが、高速なデータ通信に利用可能な方式としてはストリーム暗号方式が知られている。以下に、ストリーム暗号方式の一形態である自己同期型ストリーム暗号方式について図３に示す暗号通信システムを例にあげて説明する。図３において、この暗号通信システムは、データストリーム（平文）を暗号化する自己同期型ストリーム暗号化方式の送信部１および暗号化されたストリーム（暗号文）を復号する自己同期型ストリーム復号化方式の受信部３とを有している。上記送信部１と受信部３とは互いに同形状の第１および第２のシフトレジスタ５、７を有し、同形状の第１および第２の非線形変換計算部９、１１を共有している。すなわち、上記送信部１では、平文Ｐｉを入力する第１の排他的論理和演算部１３に第１の非線形変換計算部９が接続され、上記第１の非線形変換計算部９に第１のシフトレジスタ５が接続され、上記第１の排他的論理和演算部１３の出力Ｃｉが伝送されると共に上記第１のシフトレジスタ５に入力される構成となってお

り．上記受信部３では，上記出力Ｃｉを入力する第２の排他的論理和演算部１５および第２のシフトレジスタ７の間に第２の非線形変換計算部１１が接続される構成となっている。

【０００３】次に，上記暗号通信システムにおける暗号通信動作について説明する。まず，上記送信部１は，平文Ｐｉをビット毎に入力すると同期信号に同期して暗号文Ｃｉがビット毎に出力される様になっている。すなわち．詳細に説明すると，上記平文Ｐｉと第１の非線形変換計算部９の出力とは上記第１の排他的論理和演算部１３でビット毎に排他的論理和演算を施され，その結果は暗号文Ｃｉとして出力されると共に．上記第１のシフトレジスタ５の最右段に入力される。上記第１のシフトレジスタ５は同期信号に同期してその記憶されている内容を１ビット左シフトし，上記第１の非線形変換計算部９は上記第１のシフトレジスタ５の各段におけるレジスタ値を非線形変換し，結果の１ビットを出力する。一方，上記受信部３は．上記送信部１から送信された暗号文Ｃｉをビット毎に入力すると同期信号に同期して平文Ｐｉがビット毎に出力される様になっている。すなわち，暗号文Ｃｉと上記第２の非線形変換計算部１１の出力とは上記第２の排他的論理和演算部１５でビット毎に排他的論理和演算を施され，その結果は平文Ｐｉとして出力されると同時に．暗号文Ｃｉは，上記第２のシフトレジスタ７の最右段に入力される。上記第２のシフトレジスタ７は同期信号に同期してその記憶されている内容を１ビット左シフトし．上記第２の非線形変換計算部１１は上記第２のシフトレジスタ７の各段におけるレジスタ値を非線形変換し．結果の１ビットを出力する。

【０００４】

【発明が解決しようとする課題】しかしながら．上記図３に示す自己同期型ストリーム暗号方式の暗号通信システムでは，暗・復号化鍵として，上記非線形変換計算部９．１１の形状を共有する必要があり．その構造は複雑で暗・復号化鍵として扱いづらいという問題があった。また．鍵同士には，ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と平文の系列とを比較した場合．その相互相関が極めて小さくなければならない性質が要求される。すなわち．暗号解読の難易度を高くするためには，鍵同士には，復号化の鍵が暗号化鍵と異なった場合，平文と全く異なった系列が生じることが必要となる。しかるに．このような性質をもった非線形変換計算部を鍵として採択する効率的な手法が存在しないといった問題があった。本発明は，上記問題に鑑みてなされたものであって．ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と平文の系列とを比較した場合，その相互相関が極めて小さくなり．かつ、鍵の設定が容易となる自己同期型ストリーム暗号方式の暗号化及び復号化装置とその方法を提供することを目的とする。

【０００５】

【課題を解決するための手段】上記目的を達成するために．本発明は．伝送情報（平文）を暗号化する自己同期型ストリーム暗号化装置において、同期信号に同期して動作する複数段のシフトレジスタと．多ビット入力１ビット出力の非線形変換計算部と、暗号化鍵設定部と、上記シフトレジスタの一部もしくは全部のレジスタ値に対して上記暗号化鍵設定部に設定された暗号化鍵をビット毎に排他的論理和演算して上記非線形変換計算部へ供給するための第１の排他的論理和演算手段と、上記平文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算するための第２の排他的論理和演算手段とを具備し、上記非線形変換計算部は、少なくともＢｅｎｔ関数と呼ばれる多ビット入力１ビット出力のブール関数演算手段を備えたものであり、暗号文が、平文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算することによって得られ、その暗号文が、同時に上記シフトレジスタに入力される構成となっていることを特徴とする。

【０００６】本発明の他の特徴は、暗号文を復号化する自己同期型ストリーム復号化装置において、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力１ビット出力の非線形変換計算部と、復号化鍵設定部と．上記シフトレジスタの一部もしくは全部のレジスタ値に対して上記復号化鍵設定部に設定された復号化鍵をビット毎に排他的論理和演算して上記非線形変換計算部へ供給するための第１の排他的論理和演算手段と、暗号文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算するための第２の排他的論理和演算手段とを具備し．上記非線形変換計算部は、少なくともＢｅｎｔ関数とよばれる多ビット入力１ビット出力のブール関数演算手段を備えたものであり．上記暗号文が、上記シフトレジスタに入力され、同時に．上記平文が、先の暗号文と非線形変換計算部からの出力とをビット毎に排他的論理和演算を施すことによって得られることである。本発明の他の特徴は．伝送情報（平文）を暗号化する暗号化方法であって、同期信号に同期して動作する複数段のシフトレジスタの一部もしくは全部のレジスタ値に対して暗号化鍵設定部に設定された暗号化鍵を第１の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、少なくともＢｅｎｔ関数と呼ばれる多ビット入力１ビット出力のブール関数演算手段を備えた非線形変換計算部によって上記第１の排他的論理和演算手段よりの値を非線形変換するステップと、上記平文と上記非線形変換計算部からの出力とを第２の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、上記暗号文を上記シフトレジスタに入力するステップとを具備することである。

【０００７】本発明の他の特徴は、暗号文を復号化する復号化方法であって、同期信号に同期して動作する複数

段のシフトレジスタの一部もしくは全部のレジスタ値に対して復号化鍵設定部に設定された復号化鍵を第１の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと．少なくともＢｅｎｔ関数とよばれる多ビット入力１ビット出力のブール関数演算手段を備えた非線形変換計算部によって上記第１の排他的論理和演算手段よりの値を非線形変換するステップと、上記暗号文と上記非線形変換計算部からの出力とを第２の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、上記暗号文を．上記シフトレジスタに入力するステップとを具備することである。

【０００８】

【発明の実施の形態】以下．本発明を図示した実施形態に基づいて説明する。図１は、本発明による通信システムの一実施形態を示す構成図である。図１に示す様に、この暗号通信システムは．データストリーム（平文）を暗号化する自己同期型ストリーム暗号化方式の送信部（暗号化装置）１７および暗号化されたストリーム（暗号文）を復号する自己同期型ストリーム復号化方式の受信部（復号化装置）１９とから成っている。上記送信部１７と受信部１９とは互いに同形状のシフトレジスタ２１．２３を有し．同形状の非線形変換計算部２３．３７を共有する。すなわち、上記送信部１７では、平文Ｐｉを入力する第２の排他的論理和演算部２１に第１の非線形変換計算部２３が、上記第１の非線形変換計算部２３に第１の排他的論理和演算部群２５が接続され．上記第１の排他的論理和演算部群２５に暗号化鍵設定部２７および第１のシフトレジスタ２９が接続され、上記第１の排他的論理和演算部２１の出力Ｃｉが暗号文として伝送されると共に上記第１のシフトレジスタ２９へ入力される構成となっている。

【０００９】上記受信部１９では、上記出力Ｃｉを入力する第４の排他的論理和演算部３１および第２のシフトレジスタ３３の間に第３の排他的論理和演算群３５および第２の非線形変換計算部３７が接続されており．上記第３の排他的論理和演算部群３５のもう一方には復号化鍵設定部３９が接続されている。そして、ここで上記送信部１７と受信部１９とがそれぞれ暗号化鍵設定部２７．復号化鍵設定部３９に同じ値を共有した場合．以下のように暗号通信が成立する。上記送信部１７では、平文Ｐｉをビット毎に入力すると同期信号に同期して暗号文Ｃｉがビット毎に出力される。詳細を説明すると、平文Ｐｉと上記第１の非線形変換演算部２３の出力は第２の排他的論理和演算部２１でビット毎に排他的論理和演算を施され、その結果は暗号文Ｃｉとして出力されると共に．第１のシフトレジスタ２９の最右段に入力され、＊

$$S_i = (S_{i,1}, \cdots, S_{i,n}), S_{i,j} \in \{0,1\}, (1 \le j \le n)$$

で表し、上記非線形変換計算部（Ｂｅｎｔ関数）２３の入力を、

＊上記第１のシフトレジスタ２９は同期信号に同期してその記憶されている内容を１ビット左シフトする．上記第１の非線形変換計算部２３には上記第１のシフトレジスタ２９の各段におけるレジスタ値に対して、上記暗号化鍵設定部２７に設定された値とビット毎に上記第１の排他的論理和演算部群２５によって排他的論理和演算を施された値が入力され、それらが非線形変換され．結果の１ビットが出力される。

【００１０】上記受信部１９では、上記送信部１７から送信された暗号文Ｃｉをビット毎に入力すると同期信号に同期して平文Ｐｉがビット毎に出力される。詳細を説明すると、暗号文Ｃｉと第２の非線形変換演算部３７の出力とは第４の排他的論理和演算部３１でビット毎に排他的論理和演算を施され．その結果は平文Ｐｉとして出力される。同時に暗号文Ｃｉは第２のシフトレジスタ３３の最右段に入力され、第２のシフトレジスタ３３は同期信号に同期してその記憶されている内容を１ビット左シフトする。上記第２の非線形変換計算部３９には上記第２のシフトレジスタ３３の各段におけるレジスタ値に対して、復号化鍵設定部３９に設定された値とビット毎に第３の排他的論理和演算部群３５によって排他的論理和演算を施された値が入力され、それらが非線形変換され．結果の１ビットが出力される。ここで、上記非線形変換計算部２３．３７はＢｅｎｔ関数と呼ばれる多ビット（偶数ビット）入力１ビット出力のブール関数の演算部からなり、当然のことながら、両者は全く同一のＢｅｎｔ関数に基づき構成したものである。その一例を図２に示す。すなわち、図２に示す様に．このブール関数演算部では、入力端子４１～４７を通じて入力されたビット値が論理積演算部４９．５１で論理積演算され．その後に．それぞれ排他的論理和演算部５３に入力され、排他的論理和演算が施され．その結果が出力端子５５に出力される。また．同じ値を上記暗号化鍵設定部２７および復号化鍵設定部３９で共有する様にしている。

【００１１】以上のように構成された自己同期型ストリーム暗号方式の通信システムにより暗号通信を行った場合．ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列を．平文の系列と比較した場合、その相互相関が極めて小さくなる性質を有するわけであるが．その理由について以下に説明する。いま．図１の自己同期型ストリーム暗号方式の通信システムにおける送信部において．時刻ｉで入力される平文をＰｉ．出力される暗号文をＣｉ、第１のシフトレジスタ２９の出力を．

【数１】

$$\cdots\cdots(1)$$

【数２】

$$\mathbf{x}_i = (x_{i,1},\cdots,x_{i,n}),\ x_{i,j} \in \{0,1\},(1 \le j \le n) \quad \text{.....(2)}$$

上記非線形変換計算部２３の出力を、

$$z_i = f(\mathbf{x}_i) \in \{0,1\} \quad \text{.....(3)}$$

で表したとする。ただし、ｎは偶数である。このとき、上記暗号化鍵設定部２７に設定される暗号化鍵を、

$$\mathbf{k} = (k_1,\cdots,k_n),\ k_j \in \{0,1\},(1 \le j \le n) \quad \text{.....(4)}$$

とすれば、

$$\mathbf{x}_i = \mathbf{s}_i \oplus \mathbf{k} \quad \text{.....(5)}$$

となる。ただし、

$$\mathbf{s}_i \oplus \mathbf{k} = (s_{i,1} \oplus k_1,\cdots,s_{i,n} \oplus k_n) \quad \text{.....(6)}$$

であり、＋は排他的論理和演算を示す。また、暗号文ｃ$_i$は、

$$c_i = p_i \oplus f(\mathbf{x}_i) = p_i \oplus z_i \quad \text{.....(7)}$$

によって計算される。そして、これら暗号文が第１のシフトレジスタ２９に入力されるため、第１のシフトレジスタ２９においては、その内部状態は、

$$\mathbf{s}_i = (c_{i-1},\cdots,c_{i-n}) \quad \text{.....(8)}$$

と表すことができる。いま、平文ｐ$_i$同士が統計的にランダムであり、時間的にも相関が全くないと仮定すると、上記（７）式より、暗号文ｃ$_i$同士も統計的にランダムとなり、また、時間的にも相関がないことになる。これは、いかなる情報源からの系列であってもランダムな情報源からの系列と排他的論理和演算を施せばランダムな系列となるという事実から容易に理解できる。

【００１２】次に、上記受信部１９において、時刻$_i$に

$$p_i = c_i \oplus z_i = c_i \oplus f(\mathbf{x}_i) \quad \text{.....(9)}$$

上記（９）式に上記（５）、（６）式および上記（８）式を適用すれば次式を得る。

$$p_i = c_i \oplus f(c_{i-1} \oplus k_1,\cdots,c_{i-n} \oplus k_n) \quad \text{.....(10)}$$

いま、上記復号化鍵設定部３９に暗号化に用いた鍵と異なる鍵、

$$\mathbf{k}' = (k_1',\cdots,k_n'),\ k_j' \in \{0,1\},(1 \le j \le n) \quad \text{.....(11)}$$

を設定したとする。このとき、上記受信部１９の出力ｐ'$_i$は次式のように表される。

$$p_i' = c_i \oplus f(c_{i-1} \oplus k_1',\cdots,c_{i-n} \oplus k_n') \quad \text{.....(12)}$$

ここにｐ$_i$とｐ'$_i$の相互相関は、

$$p_i \oplus p_i' = f(c_{i-1} \oplus k_1,\cdots,c_{i-n} \oplus k_n) \oplus f(c_{i-1} \oplus k_1',\cdots,c_{i-n} \oplus k_n') \quad \text{.....(13)}$$

における１、０の出現頻度によって観測することができる。特に、１、０の出現頻度が等しければ相互相関はな

$$(c_{i-1} \oplus k_1,\cdots,c_{i-n} \oplus k_n) = (u_{i,1},\cdots,u_{i,n}) = \mathbf{u}_i \quad \text{.....(14)}$$

いことになる。上記（１３）式は、

9 10

とおくことにより、次式となる。 ＊ ＊【数１５】

$$p_i \oplus p_i' = f(\mathbf{u}_i) \oplus f(\mathbf{u}_i \oplus \mathbf{b}) \quad \text{.....(15)}$$

ただし、 ※ ※【数１６】

$$b = (b_1, \cdots, b_n) = (k_1 \oplus k_1', \cdots, k_n \oplus k_n') \quad \text{.....(16)}$$

である。ここに、ｆはＢｅｎｔ関数である。Ｂｅｎｔ関数においては、以下の性質が知られている。Ｂｅｎｔ関★数ｆにおいては、★【数１７】

$$\sum_{x \in \{0,1\}^n} f(x) \oplus f(x \oplus a) = 2^{n-1} \quad \text{.....(17)}$$

なる性質がある。ただし、

$$a \in \{0,1\}^n$$

である。この事実は、Seongtack Chee, Sangjin Lee, Kwangjo Kim等の論文、"Semi-bent functions," Advances in Cryptology ASIACRYPT'94, LNCS914, Springer-Verlag,pp.107-118,1995、等に記されている。

【００１３】上記の事実を踏まえた上で、前に述べたよ☆うに、平文ｐｉ同士が統計的にランダムであり、時間的にも相関が全くないと仮定すると、$c_{i,1}$、…、$c_{i,n}$は統計的にランダムであり、時間的にも相関が全くないことになるから、上記式（１５）におけるｕｉもランダムとみなせることになる。従って、上記式（１５）に上記式（１７）の結果を適用することにより、

【数１８】

$$\sum_{i=1}^{x} p_i \oplus p_i' = \sum_{i=1}^{x} f(\mathbf{u}_i) \oplus f(\mathbf{u}_i \oplus \mathbf{b}) = 2^{n-1} \quad \text{.....(18)}$$

が得られる。これは、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列を、平文の系列と比較した場合、その相互相関が極めて小さくなることを示す。従って、上記図１に示した自己同期型ストリーム暗号方式の暗号通信システムでは、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と平文の系列とを比較した場合、その相互相関が極めて小さくなければならない条件が満たされ、暗号解読の難易度を高くすることができ、また、同じ値を共有する暗号化鍵設定部および復号化鍵設定部を設ける様にしたので、鍵の設定も容易となる。

【００１４】

【発明の効果】本発明は、以上説明したように、通信システムの送信部の非線形変換計算部が、Ｂｅｎｔ関数とよばれる多ビット入力１ビット出力のブール関数の演算部であり、暗号文は、平文と非線形変換部からの出力とをビット毎に排他的論理和演算を施すことによって得、その暗号文は、同時にシフトレジスタに入力される構成となっており、受信部の非線形変換計算部も、送信部と同じＢｅｎｔ関数と呼ばれる多ビット入力１ビット出力のブール関数の演算部であり、暗号文は、シフトレジスタに入力され、同時に、平文は、先の暗号文と非線形変換部からの出力とをビット毎に排他的論理和演算を施すことによって得る構成となっているので、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と、平文の系列とを比較した場合、その相互相関が極めて小さくなる。また、同じ値を共有する暗号化鍵設定部および復号化鍵設定部を上述した如く設ける様にしたので、鍵の設定が容易となる等の効果がある。

【図面の簡単な説明】

【図１】本発明による暗号通信システムの一実施形態を示す構成図である。

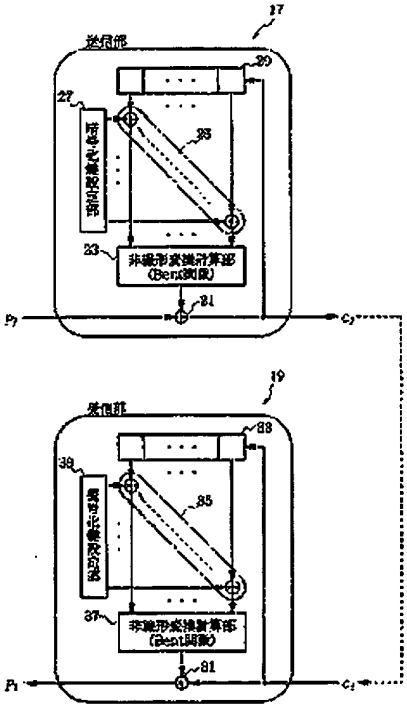
【図２】図１に示した非線形変換計算部の一例の概略構成図である。

【図３】従来の暗号通信システムの構成図である。

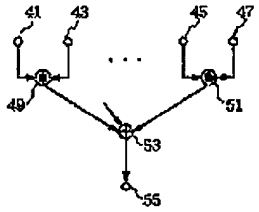
【符号の説明】

１．１７…送信部、３．１９…受信部、５、７．２９、３３…シフトレジスタ．９、１１．２３、３７…非線形変換計算部．１３、１５．２１．３１…排他的論理和演算部、２５．３５…排他的論理和演算部群．２７…暗号化鍵設定部、３９…復号化鍵設定部．４１～４７…Ｂｅｎｔ関数入力端子、４９、５１…論理積演算部、５３…排他的論理和演算部．５５…Ｂｅｎｔ関数出力端子、

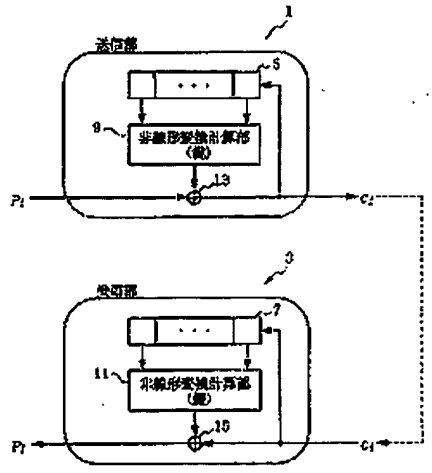
【図１】


17
送信部
20
27
35
23
非線形変換計算部
(Benett関数)
31
P_T
C_T
19
受信部
33
38
35
37
非線形変換計算部
(Benett関数)
31
P_R
C_R

【図２】


41
43
45
47
49
51
53
55

【図３】


1
送信部
5
9
非線形変換計算部
(鍵)
13
P_t
C_t
3
受信部
7
11
非線形変換計算部
(鍵)
15
P_r
C_r